REMARKS

Claims 1, 6 - 7, 9 - 11, 13, 18 - 19, 21 - 23, 25, 30, 32, 34 - 36, 39, 44, and 47 have been amended herein. Claims 31 and 45 have been cancelled herein, and Claims 48 - 52 have been added. No new matter has been introduced with these amendments or added claims, all of which are supported in the specification as originally filed. Claims 1 - 2, 6 - 7, 9 - 14, 18 - 19, 21 - 26, 30, 32, 34 - 37, 39 - 40, 44, and 47 - 52 are now in the application.

I. Rejection under 35 U.S.C. §112, second paragraph

Page 6, lines 19 - 21 of the Office Action dated August 10, 2005 (hereinafter, "the Office Action") state that Claims 1 - 2, 6 - 7, 9 - 14, 18 - 19, 21 - 26, 30 - 32, 34 - 37, 39 - 40, 44 - 45, and 47 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as his invention. Appropriate amendments have been made herein, and the Examiner is respectfully requested to withdraw the §112 rejection.

II. Rejection under 35 U.S.C. §102(b)

Page 7, lines 22 - 24 of the Office Action state that Claims 13 - 14, 18 - 19, 21 - 22, 24 - 26, 30 - 32, 34 - 35, 37, 39 - 40, 44 - 45, and 47 are rejected under 35 U.S.C. §102(b) as being anticipated by Patel et al ("An Efficient Discrete Log Pseudo Random Generator"). Claims 31 and 45 have been cancelled from the application without prejudice, rendering the rejection moot as to those claims. This rejection is respectfully traversed with regard to the remaining ones of these claims.

Applicant's independent Claims 1, 13, 25, and 39 explicitly specify "an input value comprising C random bits" (Claim 13, line 3, emphasis added), which is provided "as a short exponent x of a 1-way function G**x mod P" (Claim 13, lines 4 - 5, emphasis added). This 1-way function "generat[es] an output sequence comprising N pseudo-random bits" (Claim 13, lines 4 - 5). The N bits are "separat[ed] ... into a C-bit portion and an (N-C)-bit portion" (Claim 13, lines 9 - 10). The C-bit portion is used "as the provided input value for [i.e., as an *exponent* of; see Claim 13, line 5] a next iteration of [the function]" (Claim 13, lines 11 - 12) and the (N-C)-bit portion is used "as pseudo-random output bits" (Claim 13, lines 12 - 14).

With reference to independent Claim 13, pages 8 - 9 of Office Action provide a number of citations of Section 5 of Patel. However, the "NEW GENERATOR" described in Patel's Section 5 (see p. 313, last paragraph) describes use of an N-bit exponent, as has been discussed in detail in Applicant's prior response transmitted on June 6, 2005 (hereinafter, "Applicant's prior response), which is hereby incorporated herein by reference. Patel's use of an N-bit exponent (which is a long exponent) is patentably distinct from Applicant's claimed use of a short, C-bit exponent.

Furthermore, Applicant respectfully submits that while Patel discusses producing "n - c" bits per iteration of his generator, there is no teaching in Patel that any "c" of those bits are used as the exponent in a next-sequential iteration of the generator, in contrast to Applicant's claimed invention.

The Office Action provides a number of citations to Section 5.1 of Patel, and refers to Patel's discussions of a "short exponent". Applicant respectfully notes that Patel's discussions of "s", which is of size $\omega(\log n)$ bits, does not pertain to Patel's generator but rather pertains to his proof of security of that generator. See Section 5.1, "Proof of Security", on p. 314 of Patel. Applicant respectfully submits that the letter "s", as used by Patel, is a shorthand signal which indicates that Patel is discussing "security" of his generator.

Patel's Section 5.1 discusses how to prove that Patel's generator is secure -- that is, whether the pseudo-random bits look random. If pseudo-random bits generated by a generator are distinguishable from truly random bits, then the generator is not secure. In the general case, a proof of security presents a problem, such as factoring large numbers or discrete logarithm with short exponents, and presumes that this problem is hard to solve. An algorithm (such as a pseudo-random generator) based on this hard-to-solve problem is secure if the problem cannot be solved (or is computationally infeasible to solve). By contrast, if the problem can be solved, then the algorithm is not secure.

In Patel's paper, the problem addressed in Section 5.1 is to solve Y = G**S where S is a C-bit number. That is, given a value Y and a generator G used to compute that value Y, the problem is to find S. If S can be found, then the function is not a 1-way function and is not secure. (As will be obvious, if S is a full N-bit number, in contrast to Patel's teaching of using a C-bit number in the proof of security, then solving for an N-bit S is even more difficult than solving for a C-bit value of S. Thus, Patel must explicitly make the assumption about using

shorter exponents, for his proof of security.)

Section 5.1 thus shows how a procedure that distinguishes the bits generated by Patel's algorithm from truly random bits (i.e., that demonstrates that the bits are not pseudo-random) can find the value of S, when given the value Y that was generated when using S as an exponent. And as noted above, this further establishes that the function Y is not a 1-way function and is not secure. See the second paragraph of Section 5.1, "Now we note that we can use this to discover s given $g^s \bmod p$ [i.e., g**s mod p] where s has $\omega(\log n)$ bits". That is, Patel teaches that if s is restricted to $\omega(\log n)$ bits, then the value of S can be discovered.

This is in contrast to Applicant's claimed invention, which specifies that N pseudo-random bits are generated when using a short, C-bit exponent (Claim 13, lines 4 - 5). In other words, Applicant's independent claims specify a secure, 1-way function.

Applicant's independent claims further specify that an (N-C)-bit portion of the generated N-bit pseudo-random output sequence are used "as pseudo-random output bits" (Claim 13, lines 12 - 14). Patel similarly discusses outputting "$n - \omega(\log n)$ bits". See p. 313, final sentence discussing "NEW GENERATOR", and Section 7.1, final sentence of first paragraph ("The output of the generator are the trailing $n - \omega(\log n)$ bits of x_i ..."). However, while Applicant's claims specify using, "as the provided input value [i.e., as a short exponent; see Claim 13, line 5] for a next iteration of the [generator]" (Claim 13, lines 11 - 12), a C-bit portion of the N bits that were generated, Patel's NEW GENERATOR uses $n - \omega(\log n)$ bits as output but teaches using

all N of the bits as the exponent. Refer again to Applicant's prior response, where this N-bit exponent was discussed in detail.

Applicant notes that Patel begins the analysis of his generator in Section 7.1 by stating "Let us focus on the mechanics of the generator" (emphasis added). In other words, Section 7.1 is the discussion of how Patel's generator works, in contrast to Section 5.1. The remaining sentences of the first paragraph of Section 7.1 discuss the permissible values of the generator G, the secret seed, the expression of the generator function, and the generator output, respectively.

Applicant further notes that the second paragraph of Section 7.1 begins by explicitly stating "... each iteration involves a large exponent ..." (emphasis added). Again, this is in contrast to Applicant's claimed use of a short exponent.

Patel then states, in the second and third sentences of Section 7.1, that a short exponent could be used for a generator, but in the fourth sentence, notes that "This raises some interesting questions", and questions identified as "Question 10" and "Question 11" are then presented. In other words, Patel admits that he does not know whether a generator thus constructed would work. In particular, Patel states (following Question 10) that "... when we restrict our exponents [to short, C-bit exponents] we no longer have a permutation. Hence the simple construction [i.e., using C-bit exponents] used here is inapplicable." (emphasis added). In other words, Patel admits that he does not know how to make the generator work if only C bits are used. Accordingly, Applicant respectfully submits that Patel's text is not enabling. If a reference is not

enabling, then it does not qualify as prior art for a §102 rejection. See ***In re Sun***, 31 USPQ 2d 1451, 1453 (Fed. Cir. 1993) (unpublished), which stated

> But to be prior art under section 102(b), a reference must be enabling. . . . That is, it must put the claimed invention in the hand of one skilled in the art.

(emphasis added). See also ***Akzo N.V. v. United States International Trade Commission***, 1 USPQ 2d 1241, 1245 (Fed. Cir. 1986), ***cert. denied***, 482 U.S. 909 (1987), which stated

> Under 35 U.S.C. §102, anticipation requires that each and every element of the claimed invention be disclosed in the prior art. . . . In addition, the prior art reference must be enabling, thus placing the allegedly disclosed matter in the possession of the public.

(emphasis added). Because Patel's discussion of using a short exponent with a generator is not enabling, and therefore cannot be used as prior art under §102, Applicant respectfully submits that Patel cannot be used to anticipate his claimed invention.

Further differences between Patel and Applicant's claimed invention will be discussed. In Section 7.1, after discussing problems with his approach, Patel goes on to say (following Question 10) that "A possible method of settling this problem [i.e., the problems that result if using only C bits for exponents] ..." is to use a "perfect extender", where "pseudo-random generation [i.e., generation of pseudo-random bits] is achieved through repeated applications of the extender to a random seed". Applicant's claimed invention, by contrast, does not require application(s) of a perfect extender. Instead, Applicant's independent claims explicitly specify "using the C-bit portion of the generated N-bit output sequence" (Claim 13, lines 11 - 12, emphasis added). In other words, in Applicant's claimed invention, the bits are "of" (i.e., taken

directly from) the generated output sequence. Because the bits are taken from the generated output sequence, this necessarily implies that the bits in Applicant's claimed approach are not modified using a perfect extender (or any other type of modifying function) in between iterations.

In addition, Patel's proof of security specifies that the short exponent is selected from the leading bits of a prior iteration, while Applicant's independent claims specify no such restriction.

In view of the above, Applicant respectfully submits that his independent Claims 1, 13, 25, and 39 are patentable over the teachings of Patel. Dependent Claims 13 - 14, 18 - 19, 21 - 22, 24 - 26, 30, 32, 34 - 35, 37, 39 - 40, 44, and 47 are therefore deemed patentable over the reference as well. The Examiner is therefore respectfully requested to withdraw the §102 rejection.

III. Rejection Under 35 U.S.C. §103(a)

Page 11, lines 14 - 16 of the Office Action state that Claims 1 - 2, 6 - 7, 9 - 12, 23, and 36 are rejected under 35 U.S.C. §103(a) as being unpatentable over Patel in view of Schneier ("Applied Cryptography"). This rejection is respectfully traversed.

Applicant's independent Claims 1, 13, 25, and 39 have been discussed above, and as has been demonstrated, Patel does not anticipate these independent claims. Accordingly, Patel cannot be combined with Schneier (assuming, *arguendo*, that such combination could be made, and that one of skill in the art would be motivated to attempt it) to render dependent Claims 2, 6 -

7, 9 - 12, 23, and 36 unpatentable. The Examiner is therefore respectfully requested to withdraw the §103 rejection.

IV. Conclusion

Applicant respectfully requests reconsideration of the pending rejected claims, withdrawal of all presently outstanding rejections, and allowance of all remaining claims at an early date.

Respectfully submitted,

Marcia L. Doubet

Marcia L. Doubet
Attorney for Applicant
Reg. No. 40,999

Customer Number for Correspondence: 43168
Phone: 407-343-7586
Fax: 407-343-7587